**BANCO HIPOTECARIO DE LA VIVIENDA**
**AUDITORÍA INTERNA**

# Informe Final TI-OP-001-2019

## AUDITORÍA SOBRE PROTOCOLOS DE SEGURIDAD EN EQUIPOS DE PRECISIÓN UBICADOS EN LA SALA DE SERVIDORES Y UPS

16/01/2020

## RESUMEN EJECUTIVO

Como parte de las áreas evaluadas en esta auditoria se localizan los principales controles que deben tomarse en cuenta para una correcta administración de los aires de precisión que se ubican en la sala de servidores de datos y en la sala de Unidades de Poder Ininterrumpido (UPS).

Dentro de los hallazgos, se encontraron debilidades sobre el seguimiento a los acuerdos de niveles de servicio detalladas en el contrato 2018CD-000075-0016400001 referente al soporte y mantenimiento de los cuatro aires de precisión.

Al valorar la normativa del Departamento de TI, se determinó que la relacionada con la administración y control de los servicios prestados por terceros, no está siendo desarrollada según dicta el procedimiento PA-GAQ-RC-PR01-IN03.

Se encontró también que la boleta de control de servicios externos DTI-INF-MC-018 relacionada con los mantenimientos preventivos y correctivos de los aires de precisión, no contiene toda la información necesaria para su respectiva valoración, previo a la aprobación del pago a los proveedores externos.

Adicionalmente, sobre el acceso efectuado en horas no laborales por los oficiales de Seguridad a la sala de servidores de datos y de UPS, el área de TI no está controlando adecuadamente los motivos de acceso, ni la correcta inclusión en las bitácoras correspondientes.

Por último, se determina que la normativa e información con la que cuentan los oficiales de Seguridad para cuando se active alguna de las alarmas de emergencia y deben ingresar a la sala de servidores o de UPS, no está actualizada según la realidad actual de la institución.

Los detalles de cada aspecto indicado en los párrafos anteriores son ampliados a en la sección de Resultados de este informe.

# INDICE

# AUDITORÍA SOBRE PROTOCOLOS DE SEGURIDAD EN EQUIPOS DE PRECISIÓN UBICADOS EN LA SALA DE SERVIDORES Y UPS

## 1. INTRODUCCIÓN

### 1.1 Justificación de la auditoría

Este estudio forma parte del Plan Anual de Trabajo de esta Auditoría Interna para el año 2019 y está fundamentado en el Artículo 31 de la Ley 7052 del Sistema Financiero Nacional para la Vivienda, en el Artículo 22 de la Ley 8292, Ley General de Control Interno, en los cuales se establece que la Auditoría Interna deberá velar y fiscalizar el uso adecuado de los recursos del BANHVI.

### 1.2 Objetivo

Evaluar los controles existentes sobre los protocolos de seguridad implementados en los equipos de precisión ubicados en la sala de servidores y de UPS.

### 1.3 Alcance

El estudio abarcó la documentación, información y procesos operativos vigentes al 31 de Agosto del 2019, relacionados con la administración y control sobre los aires de precisión.

### 1.4 Metodología de Trabajo

Se aplicó la metodología establecida en el Manual para el ejercicio de la práctica de la Auditoría Interna. Además, se aplicó el Manual de Normas Generales de Auditoría para el Sector Público emitido por la División de Fiscalización Operativa y Evaluativa. Otras normas y estándares utilizados fueron:

- ✓ Reglamento SUGEF 14-17 – COBIT 5
- ✓ Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE).
- ✓ Ley General de Control Interno.
- ✓ Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE).
- ✓ Normas Generales de Auditoria para el Sector Publico

- ✓ Normativa Interna vigente (Metodología, Manuales, Políticas, Procedimientos, Instructivos y formularios)
- ✓ Norma 308 Comunicación de resultados.
- ✓ ISO/IEC 27002:2016 Tecnologías de la información – Código de buenas prácticas para controles de seguridad de la información

Además, se aplicaron técnicas de auditoría comúnmente aceptadas como entrevistas, revisión documental de la gestión administrativa y visitas de campo para la verificación del control interno.

Específicamente se ejecutaron entrevistas con los funcionarios que tienen relación directa con la administración y control de los aires de precisión, tanto a nivel del Departamento de Tecnologías de Información, como de los oficiales encargados de Seguridad del edificio. Adicional se evaluó la existencia y razonabilidad de la documentación formal y procesos establecidos sobre este tema.

Los resultados de las pruebas ejecutadas y demás documentos que respaldan el trabajo realizado, se mantienen como papeles de trabajo en el expediente electrónico de la Auditoría Interna. Las deficiencias detectadas, tanto en aspectos de control interno como operativas, de la presente revisión, se detallan en la siguiente sección de Resultados de la Evaluación.

## 2. RESULTADOS DE LA EVALUACIÓN

### *2.1* Contrato sobre el mantenimiento de los Aires de Precisión

En el proceso de auditoría se determinó que el Banco cuenta con el contrato número **2018CD-000075-0016400001** referente al soporte y mantenimiento de los cuatro aires de precisión que existen, dos previstos en la sala de servidores y los dos restantes en la sala de UPS (Unidades de Poder Ininterrumpido). Estos aires son vitales para la continuidad de los equipos tecnológicos ubicados en ambas salas y de ahí la importancia de que se mantengan en óptimas condiciones de funcionamiento.

Según consta en el punto 2 de las condiciones técnicas del contrato indicado, siempre que se efectúen los mantenimientos preventivos deberían de contemplarse al menos nueve actividades mínimas de control que deben ser corroboradas por el área de Soporte Técnico del Departamento de TI. Estas actividades fueron remitidas a la Gerencia General directamente por el Departamento de TI según memorando DTI-ME-0108-2018 del 28 de Junio del 2018 y se detallan seguidamente:

- ✓ Revisión de los filtros de aire en el evaporador.
- ✓ Revisión del sistema de humidificación.
- ✓ Revisión de rodamientos.
- ✓ Revisión del canister.
- ✓ Revisión del visor del nivel de líquido refrigerante.
- ✓ Revisión del sistema de deshumidificación.
- ✓ Revisión del sistema blower drive.
- ✓ Revisión del aislamiento interior de la unidad.
- ✓ Revisiones eléctricas de operación.

Al evaluar el cumplimiento de este apartado con la funcionaria Marcela Pavón, misma que funge como contraparte interna para aprobar los cumplimientos de los trabajos efectuados en los aires de precisión, se encontró que desconocía de la existencia de dichos controles y que los mismos debían ser incluidos en cada mantenimiento preventivo, por lo que nunca fueron valorados en su totalidad para la aceptación y respectiva aprobación de los pagos a la empresa externa, los cuales tienen un promedio mensual de $1.712.

El punto 1.5 referente a las responsabilidades de los funcionarios sobre el Sistema de Control Interno, del Manual de Normas de Control Interno para el Sector Público de la Contraloría General de la República N-2-2009-CO-DFOE, indica lo siguiente:

> *“De conformidad con las responsabilidades que competen a cada puesto de trabajo, los funcionarios de la institución deben, de manera oportuna, efectiva*

> *y con observancia a las regulaciones aplicables, realizar las acciones pertinentes y atender los requerimientos para el debido diseño, implantación, operación, y fortalecimiento de los distintos componentes funcionales del SCI."*

En el artículo 2.5.1 referente a la delegación de funciones del Manual de Normas de Control Interno N-2-2009-CO-DFOE de la Contraloría General de la República (CGR), encontramos el siguiente enunciado:

> *"El jerarca y los titulares subordinados, según sus competencias, deben asegurarse de que la delegación de funciones se realice de conformidad con el bloque de legalidad, y de que conlleve la exigencia de la responsabilidad correspondiente y la asignación de la autoridad necesaria para que los funcionarios respectivos puedan tomar las decisiones y emprender las acciones pertinentes."*

Según lo detallado por la señorita Pavón, el motivo de que no haya incluido los temas de control detallados anteriormente en las revisiones preventivas de los aíres ubicados en la sala de UPS y sala de Servidores, se debe a que cuando se le asigno la tarea de contraparte técnica en este proceso, nunca se le comunicó que tales aspectos debían ser verificados. Adicionalmente, esta actividad no se localizó como parte de las funciones propias del puesto.

Además de un incumplimiento con el contrato vigente, el no revisar cada uno de los nueve puntos de control que fueron incluidos como parte del mantenimiento de los aires de precisión, puede traer como consecuencia fallos en el servicio de estos equipos, tal como sucedió años atrás con los aires acondicionados anteriores, donde se vio afectada la continuidad operativa del Banco debido a que dichos aires no funcionaron correctamente. Así mismo, se podría estar incurriendo en una pérdida económica al no recibir todas las actividades previstas en el contrato.

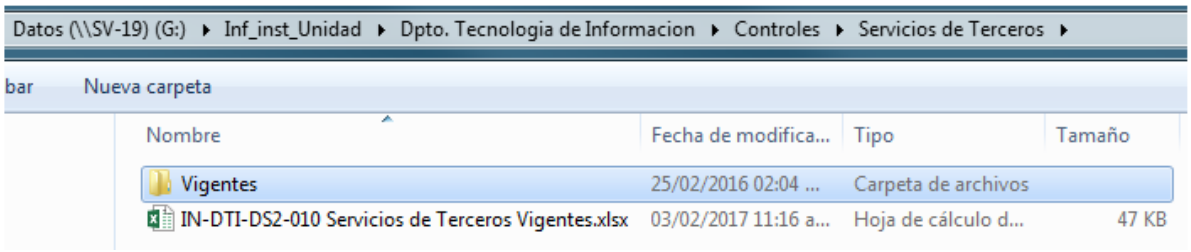
## *2.2* Servicios prestados por Terceros (PA-GAQ-RC-PR01-IN03)

Como parte de los procedimientos vigentes del Departamento de TI, se encuentra el procedimiento PA-GAQ-RC-PR01-IN03, el cual tiene como finalidad verificar que el servicio externo prestado por los proveedores, ya sea para proyectos de TI en ejecución o Contratos de Servicios, Soporte o Mantenimiento previamente suscritos con el BANHVI; se ajusten a los acuerdos de niveles de servicio (SLAs) establecidos por ambas partes en los respectivos contratos. Como parte de los controles definidos en este procedimiento, se indica en el primer punto lo siguiente:

| Actividad | Responsable | Descripción de la actividad |
|---|---|---|
| *1. Revisar servicio.* | *Ingeniero de Soporte o Sistemas* | *El Ingeniero de Soporte o Sistemas revisa que el servicio externo a realizar se ajuste con los SLA establecidos. Consulta el documento Contratos Vigentes DTI ubicado en "G:\Inf_inst_Unidad\Dpto. Tecnologia de Informacion\Controles\Servicios de Terceros", con el objetivo de conocer, aclarar o recordar las principales cláusulas que rigen la prestación del servicio pactadas entre las partes (BANHVI y Proveedor).* |

Al evaluar si en la carpeta indicada se encontraban todos los acuerdos de niveles de servicio (SLAs) relacionados con los mantenimientos preventivos y correctivos de los aires acondicionados de precisión de la sala de servidores y sala de UPS, se encontró que el único control disponible (un archivo de Microsoft Excel denominado IN-DTI-DS2-010 Servicios de Terceros Vigentes), no es utilizado desde el 3 de Febrero del 2017 y al revisar el archivo indicado, se determinó que no existe ninguna documentación sobre los contratos vigentes de los aires de precisión. En la siguiente pantalla se muestra este detalle:

*Ilustración 1 Carpeta Contratos Vigentes*




Adicionalmente se encontraron incumplimientos del procedimiento PA-GAQ-RC-PR01-IN03 en los puntos 5, 8 y 9, debido a que, al no llevar un control detallado de los SLAs para cada contrato, no podría validarse que en los servicios ofrecidos se hayan cumplido los aspectos específicos de cada contratación, tal como sucedió con los mantenimientos preventivos de los aires de precisión mencionados en el hallazgo anterior.

| | | |
|---|---|---|
| *5. Recibir documentación.* | *Ingeniero de Soporte o Sistemas* | *El Ingeniero de Soporte o Sistemas recibe documentación con las pruebas que permitan validar la finalización del servicio. Valida que el servicio fue ejecutado según fue convenido entre las partes.* |

| | | |
|---|---|---|
| *8. Recibir reporte.* | *Coordinador de TI* | *El Coordinador de TI recibe el reporte DTI-INF-MC-018-[código de servicio externo] con la documentación adjunta y valida que el servicio se haya ejecutado de conformidad con los alcances contractuales establecidos previamente. De estar todo correcto firma el reporte DTI-INF-MC-018-[código de servicio externo].*<br>*-Si hay que gestionar un pago al proveedor, inicia la gestión de pago al proveedor*<br>*-Si no hay que gestionar pago pero existe un incumplimiento por parte del proveedor, comunica a la jefatura para el trámite correspondiente ante el Área de Proveeduría.*<br>*-Si no aplica ningún pago (atención de garantía) y no existe ningún incumplimiento por parte del proveedor, escanea los documentos y los incluye en la carpeta correspondiente "G:\Inf_inst_Unidad\Dpto. Tecnologia de Informacion\Controles\Servicios de Terceros\Vigentes\NUMERO EXPEDIENTE CONTRATACION".* |
| *9. Analizar documentación* | *Jefatura de TI* | *La Jefatura de TI analiza documentación del servicio externo realizado: factura, contrato, orden de compra e informe DTI-INF-MC-018, según corresponda. Dependiendo del grado de cumplimiento del objetivo, recomendará (si aplica) el pago total, parcial o no pago de la factura. En caso de que la prestación del servicio haya incumplido una o varias cláusulas, deberá notificarlo al Área de Proveeduría para lo que corresponda.*<br>*Solicita a la secretaria la confección del memorando correspondiente.* |

El punto c) del artículo 2.1 sobre el ambiente de control, del Manual de Normas de Control Interno N-2-2009-CO-DFOE de la CGR, detalla lo siguiente:

> *"El jerarca y los titulares subordinados, según sus competencias, deben establecer un ambiente de control que se constituya en el fundamento para la operación y el fortalecimiento del SCI, y en consecuencia, para el logro de los objetivos institucionales. A los efectos, debe contemplarse el conjunto de factores organizacionales que propician una actitud positiva y de apoyo al SCI y a una gestión institucional orientada a resultados que permita una rendición de cuentas efectiva, incluyendo al menos lo siguiente:*
> *(…)*
>
> *c. El mantenimiento de personal comprometido y con competencia profesional para el desarrollo de las actividades y para contribuir a la operación y el fortalecimiento del SCI."*

El punto 2 del proceso DSS01.02 relacionado con gestionar los servicios externalizados de TI, del COBIT 5, detalla:

> *"Asegurar que los requerimientos operativos del negocio y de procesamiento de TI, así como las prioridades en la entrega del servicio se adhieren y son conformes a los contratos y ANSs con terceros que alojan o proveen servicios."*

Se estima como posible causa del incumplimiento en el procedimiento PA-GAQ-RC-PR01-IN03, una falta de seguimiento y supervisión en el cumplimiento y aseguramiento de la normativa del Departamento de TI que tenga relación con los servicios prestados por terceros.

Al no llevar un pulso claro y actualizado de todos los acuerdos de niveles de servicio inherentes a cada contratación con proveedores externos, especialmente en el área de tecnología, podría verse afectada la continuidad del Banco al afectarse alguno de los servicios básicos que sean administrados por outsourcing. Además pueden existir afectaciones económicas por pago de servicios a proveedores externos que no se están cumpliendo en su totalidad.

## 2.3 Control de Servicios externos DTI-INF-MC-018

Todos los meses al efectuarse los mantenimientos preventivos de los aires de precisión de la sala de servidores y de UPS, como parte de la supervisión realizada por el personal de TI, se realiza una boleta de control de servicios externos que en el caso de los aires de precisión tiene el código DTI-INF-MC-018. Se detalla un ejemplo de este tipo de reportes:

*Ilustración 2 Formulario Control de Servicios Externos*

BANCO HIPOTECARIO DE LA VIVIENDA
Departamento de Tecnología de Información

DTI-INF-MC-018
-0961-

**Control de servicios Externos**

**Solicitud de Servicio** 20019 **Responsable:** Marcela Pavón Martínez **Fecha Servicio:** 31/10/2018 03:20:37 p.m.

**Requerimiento:** **Servicio de Contrato Aires Acondicionados Sala de SRVS y UPS Grupo Electrotécnica** Plan Táctico de TI 2018, numeral 1.3.1 Contratos de Mantenimiento anuales, Plan de Inversión Estimada, inciso c. Soporte 4 Aires Acondicionados Data Mate 3 Ton, y en seguimiento a Orden de Compra **No. 00022961**. Contratación Directa **2018CD-000075-0016400001. IDC: 29**

**Solución:** Factura 00100001010000000566. De dicha empresa. Este costo debe cargarse a la Partida Presupuestaria No. 1.08.08 Soporte 4 Aires Acondicionados Data Mate 3 Ton. Correspondiente el mes de octubre
Monto: $ 1712
TC: ¢ 600 (negociación con la empresa)
Monto: ¢ 1,027.200

**#Boleta Proveedor:** 0010000101000 0566 **Horas Efectivas:** 0 **Calificacion:** 100

----------Calificación del Servicio ---------- Tipo Servicio:S01 Soporte Técnico En Banhvi
V01: Puntualidad en el servicio, Muy Bueno De acuerdo a lo solicitado ---------- V02: Cumplimiento requerimiento, Muy Bueno De acuerdo a lo solicitado ---------- V03: Servicio en tiempo establecido, Muy Bueno De acuerdo a lo solicitado ---------- V04: Actitud del proveedor, Muy Bueno De acuerdo a lo solicitado ----------

Marcela Pavón
**Firma Responsable** **Firma Revisor**

Al evaluar los reportes del año 2018 y 2019, la gran mayoría carecen del detalle de horas efectivas en la ejecución del mantenimiento preventivo de los aires y sin embargo se pagaron en su totalidad. También, en el detalle de la solución no se indica la actividad efectuada, sino información general sobre el pago tales como montos, facturas, partidas presupuestarias, entre otros. Por último, se carece de mayor información que permita evaluar el servicio brindado.

En el punto 6 del procedimiento PA-GAQ-RC-PR01-IN03 "*Servicios prestados por proveedores externos*", encontramos la siguiente actividad:

> *"El Ingeniero de Soporte o Sistemas registra en el "Sistema de Solicitudes de Servicio", el detalle de la solución aplicada acorde con el servicio recibido y genera el código de servicio externo. Como mínimo el registro debe contener: número de Expediente de la Contratación Administrativa, motivo de la visita, fecha de visita, horas efectivas, nombre de la empresa, nombre del técnico de la empresa, especificar si es por contrato o por horas profesionales y calificación del servicio recibido acorde con las cláusulas que rigen la prestación del servicio. Cuando el proveedor incumpla una o más cláusulas contractuales que rigen la prestación del servicio, debe registrar y documentar el incumplimiento como parte de la calificación del servicio en el ítem del formulario que corresponda."* El subrayado es propio.

Adicionalmente el artículo 2.5.2 de autorización y aprobación del Manual de Control Interno N-2-2009-CO-DFOE, indica lo siguiente:

> *"La ejecución de los procesos, operaciones y transacciones institucionales debe contar con la autorización y la aprobación respectivas de parte de los funcionarios con potestad para concederlas, que sean necesarias a la luz de los riesgos inherentes, los requerimientos normativos y las disposiciones institucionales."*

El artículo 4.6 denominado "*Administración de servicios prestados por terceros*", de las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE), indica:

> *"La organización debe asegurar que los servicios contratados a terceros satisfagan los requerimientos en forma eficiente. Con ese fin, debe:*
> *a. Establecer los roles y responsabilidades de terceros que le brinden servicios de TI.*
> *b. Establecer y documentar los procedimientos asociados con los servicios e instalaciones contratados a terceros.*
> *c. Vigilar que los servicios contratados sean congruentes con las políticas relativas a calidad, seguridad y seguimiento establecidas por la organización.*

*d. Minimizar la dependencia de la organización respecto de los servicios contratados a un tercero.*
*e. Asignar a un responsable con las competencias necesarias que evalúe periódicamente la calidad y cumplimiento oportuno de los servicios contratados."*

Una de las posibles causas de que el formulario de control de servicios externos DTI-INF-MC-018 se esté utilizando sin la suficiente información, es porque desde que se implementó el control, no ha venido actualizándose con el cambio de procesos y normativa que ha tenido el Banco en los últimos dos años.

Al no tener claridad si el servicio se cumplió según lo estipulado en el respectivo contrato, además de aprobar pagos que podrían no corresponder, se podría ver afectados los insumos tecnológicos (servidores, equipos de comunicación, bases de datos, sistemas de información, entre otros) necesarios para la operativa del Banco.

## 2.4 Acceso a la sala de Servidores y UPS por personal de Seguridad

Como parte de la evaluación, se determinó que los guardas de Seguridad poseen una tarjeta y las claves respectivas para poder acceder a la sala de Servidores y de UPS, esto en caso de que en horas no laborales y sin presencia de personal de TI, se activen las alarmas de incendio, robo o aires acondicionados; situación que según lo corroborado ha sucedido en varias ocasiones en los últimos años. Al respecto se comprobó que el personal de Soporte Técnico de TI no está realizando un seguimiento sobre los días en que los oficiales ingresan a estos sitios ni de las actividades que ejecutan.

Los puntos 13 y 14 del procedimiento PA-GABS-AS-PR03-IN01 relacionado con la activación de los sistemas de alarma de incendio, robo y circuito cerrado en las instalaciones del BANHVI

*"En caso de activación de la alarma de los aires acondicionados ubicados en la sala de UPS del primer piso, sala de servidores del cuarto piso y alarma de nivel de agua del tanque de captación en horas no hábiles, el Oficial de Seguridad contactará a la empresa contratada en servicio de 24 horas para la atención de la situación (Es responsabilidad de Servicios Generales mantener el número del proveedor actualizado). Posteriormente, llamará a los números de contacto del personal de soporte de Tecnologías de Información.*
*En caso de activarse la alarma externa fuera de horario laboral, procederá a reportarlo a Soporte Crítico al número 800-2748426, indicando el Código de Servicio número AA0432.*

*El Oficial de Seguridad ingresa a la sala que presenta la alarma y presiona el botón rojo que se ubica sobre el panel AC4, para cortar el sonido de la alarma, mientras esperan a que los técnicos de Soporte Crítico se presenten a resolver el problema reportado."*

El proceso DSS01.03 denominado "*Supervisar la infraestructura de TI*", del COBIT 5, detalla el siguiente control:

*"Supervisar la infraestructura de TI y los eventos relacionados con ella. Almacenar la suficiente información cronológica en los registros de operaciones para permitir la reconstrucción, revisión y examen de las secuencias de tiempo de las operaciones y las actividades relacionadas con el soporte a esas operaciones"*

La razón del porqué el personal de Soporte Técnico no le da seguimiento al ingreso de los guardas en las zonas seguras de TI, se debe a que no está estipulado como parte de su normativa vigente, además de que no se han implementado controles automatizados que le den seguimiento al uso de la tarjeta de acceso administrada por los oficiales de Seguridad.

Al no llevar un control estricto sobre los accesos físicos de los oficiales de Seguridad a la sala de Servidores y de UPS, podrían darse ingresos injustificados y no registrados en las respectivas bitácoras de ingresos, con implicaciones negativas en la seguridad física de los equipos y por consiguiente afectaciones a nivel lógico de la información institucional.

## *2.5* Controles efectuados por el personal de Seguridad

Como parte del estudio se valoró la participación del personal de seguridad que es contratado por el Banco, específicamente lo relacionado a la atención cuando se presente alguna alarma o situación anormal tanto en la Sala de UPS como en la sala de Servidores; esto fuera de horario de oficina y cuando no se encuentren funcionarios del Departamento de Tecnologías de Información que puedan atender la emergencia. En este sentido se localizaron las siguientes anomalías:

- ✓ El punto 5.13 denominado "*Sistema de alarma sala de Servidores y UPS*", del documento Plan de Seguridad del Banco Hipotecario de la Vivienda, extraído de la Intranet institucional, detalla que en caso de activarse alguna de las alarmas de los aires acondicionados ubicados en la sala de UPS y de Servidores, en primera instancia el personal de seguridad debe llamar a la empresa contratada para reportar el problema y seguidamente llamará al personal de Departamento de TI que corresponda. Al respecto en entrevista

con el personal de Seguridad, se comprobó que, en las pasadas anomalías con la planta eléctrica, no se realizó ningún comunicado al personal del Departamento de TI y los guardas solo revisaron la sala de UPS, no así la sala de Servidores. Además, los únicos dos números de contacto de funcionarios de TI con los que cuenta el personal de Seguridad son los de Oscar Hidalgo y Edwin Vargas, mismos que no laboran para el Banco desde ya un tiempo considerable.

- ✓ Relacionado también con el documento del Plan de Seguridad del Banco, en el punto 5.13 se detalla que, al activarse la alarma de la sala de servidores y UPS, los guardas deben anotar en la bitácora al menos la hora de activación de la alarma, hora del reporte a la empresa externa y a funcionarios de TI y los nombres de las personas a quien se les dio el mensaje. Evaluando las últimas anotaciones de las bitácoras referentes con este tema, se localizó que no se está incluyendo toda la información requerida y que cada guarda la detalla según su parecer.

- ✓ Valorando los procedimientos utilizados por el personal de Seguridad que tienen visible en el cuarto de vigilancia y que están relacionados con las actividades que deben ejecutar cuando falle la planta eléctrica o los tanques de captación de agua, se evidenció que está documentación está desactualiza y que los guardas no están conscientes de la importancia que tienen los tanques de agua para el funcionamiento de los aires de precisión, por lo que se nos indicó que solo revisan la sala de servidores y de UPS cuando se den fallos en la planta eléctrica, no así si se activaran las alarmas de los tanques de agua.

El punto 9 de las actividades de control del proceso DSS01.05 relacionado con la gestión de las instalaciones del COBIT 5, indica lo siguiente:

> *"Registrar, supervisar, gestionar y resolver incidentes en las instalaciones siguiendo los procesos de gestión de incidentes de TI. Poner a disposición informes sobre incidentes en instalaciones donde la legislación y las regulaciones requieran su divulgación."*

Adicionalmente encontramos en el punto 5 de las actividades de control del proceso DSS03.01 que trata sobre identificar y clasificar los problemas, del COBIT 5:

> *"Definir e implementar criterios y procedimientos para informar de los problemas identificados, incluyendo clasificación, categorización y priorización de problemas.*
> *(…)*

*5. Informar del estado de problemas identificados al centro de servicios de forma que los clientes y la gestión de TI puedan mantenerse informados"*

En el punto 6) del artículo 16.1.1 sobre responsabilidades y procedimientos, del estándar INTE/ISO/IEC 27002:2016, se muestra el siguiente enunciado:

*"Se deberían establecer responsabilidades y procedimientos de gestión para asegurarse de tener una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.*
*(…)*
*6) procedimientos de respuesta incluyendo aquellos para el escalamiento, la recuperación controlada de un incidente y la comunicación a personas internas o externas u organizaciones;"*

Además, en el punto 16.1.2 "*Reporte de eventos de seguridad de la información*", también del estándar INTE/ISO/IEC 27002:2016, se detalla:

*"Los eventos de seguridad de la información deberían ser reportados a través de canales de gestión adecuados tan pronto como sea posible."*

Como razón principal de las situaciones indicadas con el personal de Seguridad, se denota una falta de capacitación para estos funcionarios, así como actualización en la normativa vigente desarrollada por otras unidades del Banco donde deben intervenir los guardas.

Un efecto directo de que los funcionarios de Seguridad no tengan la certeza de cómo actuar ni cuenten con los insumos de información suficientes en caso de que se presente una emergencia en la sala de servidores o de UPS en horas no hábiles, es que se puedan dañar o ver afectados los principales equipos tecnológicos del Banco, así como todos los sistemas de información que se ejecutan en estos activos.

## 3. CONCLUSIÓN

En la auditoría sobre la administración de los aires de precisión de la sala de servidores de datos y de UPS, se llega a la conclusión de que el Departamento de TI ha implementado una serie de controles a nivel de mantenimientos preventivos que dan una seguridad aceptable sobre el funcionamiento y continuidad de estos.

No obstante, a nivel normativo se determina que existen debilidades en áreas de importancia tales como los acuerdos de niveles de servicio del contrato de mantenimiento actual, procedimientos tanto del área de TI como de la Dirección Administrativa, en el formulario de control de servicios externos y en ciertas actividades de control y aseguramiento realizadas por los oficiales de Seguridad en la sala de servidores de datos y de UPS.

El trabajo se realizó aplicando las técnicas de auditoria vigentes, evaluando la normativa referente a la administración de los aires de precisión, así como los principales controles implementados sobre este tema.

## 4. RECOMENDACIONES

En relación con los informes de la Auditoría Interna dirigidos a los titulares subordinados, la Ley General de Control Interno No. 8292 en su artículo 36 establece:

*"Artículo 36. —**Informes dirigidos a los titulares subordinados**. Cuando los informes de auditoría contengan recomendaciones dirigidas a los titulares subordinados, se procederá de la siguiente manera:*

*a) El titular subordinado, en un plazo improrrogable de diez días hábiles contados a partir de la fecha de recibido el informe, ordenará la implantación de las recomendaciones. Si discrepa de ellas, en el transcurso de dicho plazo elevará el informe de auditoría al jerarca, con copia a la auditoría interna, expondrá por escrito las razones por las cuales objeta las recomendaciones del informe y propondrá soluciones alternas para los hallazgos detectados.*

*b) Con vista de lo anterior, el jerarca deberá resolver, en el plazo de veinte días hábiles contados a partir de la fecha de recibo de la documentación remitida por el titular subordinado; además, deberá ordenar la implantación de recomendaciones de la auditoría interna, las soluciones alternas propuestas por el titular subordinado o las de su propia iniciativa, debidamente fundamentadas. Dentro de los primeros diez días de ese lapso, el auditor interno podrá apersonarse, de oficio, ante el jerarca, para pronunciarse sobre las objeciones o soluciones alternas propuestas. Las soluciones que el jerarca ordene implantar y que sean distintas de las propuestas por la auditoría interna, estarán sujetas, en lo conducente, a lo dispuesto en los artículos siguientes.*

c) *El acto en firme será dado a conocer a la auditoría interna y al titular subordinado correspondiente, para el trámite que proceda."*

A continuación, se presentan las recomendaciones de acuerdo con el orden en que fueron expuestas en la sección de resultados.

### *4.1* Contrato sobre el Mantenimiento de los Aires de Precisión

**Al Departamento de TI**

4.1.1 Debe incluirse como parte de las revisiones preventivas para los aires de precisión ubicados en la sala de servidores y de UPS, cada uno de los nueve puntos de control detallados en la sección dos de las condiciones técnicas del contrato vigente. Para esto además debe actualizarse la normativa del área de Tecnologías de Información según corresponda.

Nivel de Riesgo: **Alto**

4.1.2 Implementar para las actividades o servicios de mayor riesgo a nivel de tecnologías de información, un proceso de inducción con el que se capacite formalmente a los funcionarios del Departamento de TI que se les asigne nuevas labores. Como parte de esta actividad debe evaluarse la vigencia de la normativa vigente que esté relacionada con la función que se ve a ejecutar. Adicionalmente será necesario dejar constancia de los temas tratados en la capacitación.

Nivel de Riego: **Medio**

4.1.3 Incluir en el Manual de Puestos del Departamento de TI, para el código 565 de Especialista en Redes de Comunicación de Datos, la función de controlar el cumplimiento de las cláusulas correspondientes a todos los contratos con proveedores externos, en los que dicho puesto funja como contraparte interna.

Nivel de Riego: **Alto**

### *4.2* Servicios prestados por Terceros (PA-GAQ-RC-PR01-IN03)

**Al Departamento de TI**

4.2.1 Deben efectuar las gestiones necesarias para restablecer cada uno de los controles inmersos en el procedimiento PA-GAQ-RC-PR01-IN03 relacionado con los servicios prestados por terceros a nivel tecnológico. Como parte de este estudio, debe valorarse la posibilidad de incluir controles adicionales a los existentes, para que se amolden a la realidad operativa y tecnológica de los procesos que sean coadministrados por terceras partes.

Nivel de Riesgo: **Medio**

4.2.2 Es necesario establecer algún mecanismo de control, con el cual se pueda dar un seguimiento oportuno y expedito a la aplicabilidad de las políticas, procedimientos e instructivos del Departamento de TI que fueron definidos para validar el cumplimiento de los servicios tecnológicos contratados a proveedores externos.

Nivel de Riesgo: **Medio**

### *4.3* Control de Servicios Externos DTI9-INF-MC-018

**Al Departamento de TI**

4.3.1 Se debe actualizar de acuerdo con la normativa vigente, la información presentada en el formulario de control de servicios externos DTI-INF-MC-018 utilizado por el Departamento de TI. Los datos contenidos en este formulario deben ser suficientes y correctos para que los supervisores y encargados de procesos, tengan la facilidad de revisar y aprobar los pagos por mantenimiento preventivo o correctivo que se soliciten para los proveedores externos.

Nivel de Riego: **Medio**

### 4.4 Acceso a la sala de Servidores y UPS por personal de Seguridad

**Al Departamento de TI**

4.4.1 Se debe implementar un control automatizado que de un seguimiento al uso de la tarjeta de acceso con que cuenta el personal de Seguridad del Banco para ingresar en las zonas seguras de tecnologías de información. Una vez implementado el control, se debe incluir en su normativa las verificaciones correspondientes.

Nivel de Riesgo: **Alto**

4.4.2 Debe actualizar la normativa del Departamento de TI para que se incluya la valoración de cada acceso que realicen los oficiales de Seguridad a la sala de servidores y de UPS en horas no laborales, indistintamente de que sea registrada o no en la bitácora de accesos administrada por los guardas.

Nivel de Riesgos: **Alto**

## 4.5 Controles efectuados por el personal de Seguridad

**A la Dirección Administrativa**

4.5.1 Se debe actualizar la documentación de contacto utilizada por el personal de Seguridad del Banco, específicamente los nombres y números de contacto de los funcionarios del Departamento de TI que deban ser contactados cuando se activen las alarmas de los aires de precisión y de las bombas de agua.

Nivel de Riesgo: **Medio**

4.5.2 Actualizar los procedimientos que deben ser ejecutados por los guardas de Seguridad cuando deban contactar a los proveedores externos que dan mantenimiento a los aires acondicionados de precisión. Además, debe crearse un nuevo procedimiento para cuando se activen las alarmas de las bombas de agua, ya que deben considerarse tan relevantes para la continuidad de los equipos tecnológicos como la planta eléctrica.

Nivel de Riesgo: **Alto**

4.5.3 Elaborar un formulario para ser utilizado por el personal de Seguridad en el que se incluya cada uno de los valores o información que debe ser registrada cada vez que estos funcionarios deban ingresar a la sala de Servidores o de UPS por motivos de alarmas activadas en horas no laborales. Como parte de los datos de este formulario, además de lo detallado en el punto 5.13 del Plan de Seguridad del Banco, deben incluirse al menos la firma del Coordinador del Área de Servicios Generales y alguna de las firmas del personal del Departamento de TI que funja como contraparte a nivel de control de accesos a las áreas seguras de TI.

Nivel de Riesgo: **Medio**

4.5.4 Debido a la considerable rotación de personal que tiene la empresa que da el servicio de Seguridad Institucional, debe normarse al menos una capacitación anual donde se ratifiquen los principales aspectos de seguridad relacionada con las tecnologías de información, esto en caso de que los oficiales de Seguridad tengan que ejecutar protocolos de emergencia ya sea en la sala de servidores o de UPS. Debe dejarse constancia documental de la capacitación ofrecida y esta debe incluir a todo el personal vigente. Al respecto y como parte de esta normativa, debe implementarse un proceso de inducción para el nuevo personal de seguridad donde se deje constancia de que fueron capacitados en materia de seguridad tecnológica.
Nivel de Riesgo: **Alto**

**Estudio realizado por:**

JORGE ANTONIO RAMIREZ BOLAÑOS (FIRMA)

Firmado digitalmente por JORGE ANTONIO RAMIREZ BOLAÑOS (FIRMA)
Fecha: 2020.01.15 16:56:30 -06'00'

**MATI. Jorge Ramirez Bolaños**
**Auditor Encargado**

GUSTAVO FLORES OVIEDO (FIRMA)

Firmado digitalmente por GUSTAVO FLORES OVIEDO (FIRMA)
Fecha: 2020.01.17 16:24:41 -06'00'

**Aprobado MBA Gustavo Flores Oviedo**
**Auditor Interno.**